

[NEWS] GRC.com Can be Used to Scan Arbitrary IP Addresses

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-11/0060.html>

From: support@securiteam.com

Date: 11/28/01

From: support@securiteam.com

To: list@securiteam.com

Subject: [NEWS] GRC.com Can be Used to Scan Arbitrary IP Addresses

Message-Id: <20011128070804.42B36138BF@mail.der-keiler.de>

Date: Wed, 28 Nov 2001 08:08:04 +0100 (CET)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> – Know that you're safe.

GRC.com Can be Used to Scan Arbitrary IP Addresses

SUMMARY

ShieldsUp(tm) is an application developed by Steve Gibson of Gibson Research Corporation that allows a web user to request a remote port scan of their local system via the GRC.Com web site (<https://grc.com/x/ne.dll?bh0bkyd2>). The "Probe my Ports" option performs a scan of many common TCP ports and reports the status of each port back to the user's browser.

The development of the application and its method of identifying the client IP address are quite insecure. As a result, it is possible to have ShieldsUp! perform a port scan against any other machine on the Internet and return the results to the web user. The remote system will log the scan as having originated from one of Steve Gibson's machines.

DETAILS

Gibson has chosen to use a simple hidden tag in the client-side HTML code to identify the IP address that is passed to the scanning engine. Though the client's IP address is hashed, it is trivial to alter the value of the

Securiteam: [NEWS] GRC.com Can be Used to Scan Arbitrary IP Add

hidden tag in order to request that a different IP address be scanned. The true IP address is never checked in the HTTP header during the scan – ShieldsUp happily scans the other box while returning the result set into the browser of the box that requested the scan.

Fenris, The Wolf, a member of Hammer of God, quickly reviewed the hash algorithm used to represent the IP address and found it weak; therefore, one can easily submit requests, via the Shields Up web page, for specific IP addresses to be scanned.

We can easily bypass the need to crack the hash by simply using the "IP Agent" supplied by Gibson. Over a year ago, a hacked version of IP Agent was published that allowed one to supply an address to scan— Gibson discounted this as a non-issue, but reportedly fixed IP Agent to perform a check to prevent this from happening.

However, IP Agent now supports multiple client IP addresses. One simply needs to bind the targeted IP addresses to a local interface and perform a scan request. In this case, ShieldsUp presents friendly command buttons listing the IP addresses bound to the local interfaces and allows you to select any one that you want scanned. Again, no other checking is done, and ShieldsUp will scan whatever IP address you ask it to and display the results in your own browser.

According to the scanning page, "Information gained will NOT be retained, viewed, or used by us in any way for any purpose whatsoever" this invites anyone to use Gibson's site to do port scans of other people's boxes without fear of detection.

Additionally, multiple post requests can be easily scripted to perform scans against a site in attempts to perform a denial of service attack against a host. In these cases, with sufficient requests generated, one could ask grc.com to attack another site and it will comply.

ADDITIONAL INFORMATION

The information has been provided by <mailto:magni@hammerofgod.com> Magni.

=====

This bulletin is sent to members of the SecuriTeam mailing list. To unsubscribe from the list, send mail with an empty subject line and body to: list-unsubscribe@securiteam.com In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

Securiteam: [NEWS] GRC.com Can be Used to Scan Arbitrary IP Add

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

- *Previous message:* support@securiteam.com: "[\[UNIX\] Hypermail SSI Vulnerability](#)"
- *Messages sorted by:* [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)